به نام خدا

مستند توضیحات امنیت:

۱-کلاس AES :

در ابتدا در کلاس AES دو فیلد داریم : Key & secretKey که توضیح داده می شوند:

Key: که ارایه ای از بایت هاست و در تابع setKey عملیات روی آن انجام میشود و در نهایت با پیاده سازی الگوریتم AES رو آن، secretKey ست و تنظیم می شود.

نام کلاس برگرفته از روش(AES(Advanced Encryption Standard است که عملیات رمز نگاری را در آن انجام می‌دهیم. حالا به بررسی توابع موجود در این کلاس می پردازیم:

1 - تابع SetKey(String myKey) : تابعی است که با گرفتن یک رشته از ما به عنوان کلید ابتدایی و پردازش و انجام یک سری عملیات که توضیح داده خواهند شد، در نهایت یک کلید نهایی سری را ست می کند. در ابتدا در این تابع باید از کلاس MessageDigest نمونه گیری شود و در کانستراکتور آن نوع الگوریتم برای عمل رمز نگاری را مشخص شود. سپس با توابع و متد های متنوع موجود در کلاس MessageDigest یک کلید جدید بسازیم.(توابعی نظیر -(Array.copyof(key,newLength یا (digest(key

2 - تابع getSecretKeyByToken(String token) : این تابع با گرفتن توکن ار هر کاربر که یک عدد یکتاست و انجام عملیات روی رشته توکن ، یک کلید ثانویه می سازد.(عملیات را طوری ترتیب می دهیم که به سادگی قابل ردیابی نباشد.)

3 - تابع encrypt(String strToEncrypt,secretKey) : آرگومان اول این تابع، رشته ای است که قرار است کد گذاری شود. رشته دوم، همان کلید ثانویه ای است که در تابع getSecretKeyByToke ساخته شد. سپس تابع SetKey را با ورودی secretKey صدا میزنیم. در این تابع، از کلاس Cipher استفاده شده است که بعدا به آن خواهیم پرداخت.

4 - تابع decrypt(String strToDecrypt,secretKey) : همان کار های encrypt را انجام میدهد با این تفاوت که کدگشایی می کند و عملیات برعکس است.

۲-کلاس Cipher:

این کلاس برای عملی ساختن encryption & decryption ساخته شده است. در ابتدا باید یک نمونه از آن گرفته شود و در سازنده آن نوع الگوریتم را مشخص کنیم. سپس باید تابع init را صدا بزنیم که ساز و کار آن مطابق شکل زیر است:

Init(Cipher_Mode,String secretKey)

که secretKey درآن برابر همان کلیدی است که در تابع setKey آنرا مشخص و ست کرده ایم. سپس با تابع doFinal رشته نهایی را بر میگردانیم.